



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

March 10, 2016

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2016-048

DATE(S) ISSUED:

03/10/2016

SUBJECT:

Vulnerability in PHP Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in PHP, which could allow an attacker to execute remote code. PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications. Successful exploitation of this vulnerability could allow a remote attacker to execute remote code in the context of the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation will likely result in a denial-of-service condition.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild. However, there are reports of proof-of-concept code, but it has not been made publicly available.

SYSTEM AFFECTED:

- PHP 5.6 prior to 5.6.19
- PHP 5.5 prior to 5.5.33

RISK:**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in PHP, which could allow an attacker to execute remote code. This vulnerability exists due to a use-after-free error in the 'ext/wddx/wddx.c' file, which is caused as it fails to correctly implement Web Distributed Data eXchange (WDDX) deserialization. Failed exploitation will result in a denial-of-service condition. Successful exploitation could be performed via a specially crafted XML file.

WDDX is an XML-based technology that enables complex-data exchange between various supported Web programming languages, by allocating a specific module for each supported language. The module will translate (serialize) the native data structures into an abstract form represented as XML, or de-serialize the WDDX XML into a native data structure.

Successful exploitation of this vulnerability could allow a remote attacker to execute remote code in the context of the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation will likely result in a denial-of-service condition.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade to the latest version of PHP immediately, after appropriate testing.
- Apply the principle of Least Privilege to all systems and services.

- Do not open email attachments from unknown or untrusted sources.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Limit user account privileges to only those required.

REFERENCES:

PHP:

<https://bugs.php.net/bug.php?id=71587>

<http://php.net/ChangeLog-5.php#5.6.19>

<http://php.net/ChangeLog-5.php#5.5.33>